

10 MAY 2001

09/831491

2100 Pennsylvania Avenue, NW  
Washington, DC 20037-3213

T 202.293.7060

F 202.293.7860

www.sughrue.com



Sughrue

SUGHRUE MION ZINN MACPEAK &amp; SEAS, PLLC

May 10, 2001

**BOX PCT**Commissioner for Patents  
Washington, D.C. 20231PCT/SG98/00088  
-filed November 10, 1998

Re: Application of Teow Hin NGAIR  
A METHOD OF ENCRYPTION AND APPARATUS THEREFOR  
**Assignee: KENT RIDGE DIGITAL LABS**  
Our Ref: Q64409

Dear Sir:

Applicant herewith submit the attached papers for purpose of entering the National Stage under 35 U.S.C. § 371 and in accordance with Chapter II of the Patent Cooperation Treaty: A Preliminary Amendment is attached herewith.

It is assumed that copies of the International Application, the International Search Report, the International Preliminary Examination Report, and any Articles 19 and 34 amendments as required by § 371(c) will be supplied directly by the International Bureau, but if further copies are needed, the undersigned can easily provide them upon request.

Assignment for published patent application is: **KENT RIDGE DIGITAL LABS.**

The Government filing fee is calculated as follows:

Total claims	20	-	20	=		x	\$18.00	=	\$0.00
Independent claims	3	-	3	=		x	\$80.00	=	\$0.00
Base Fee									\$1000.00

**TOTAL FEE** \$1000.00

A check for the statutory filing fee of \$1000.00 is attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16, 1.17 and 1.492 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

There is no claim to priority.

Respectfully submitted,

*Alan V. Kasper*  
for Alan V. Kasper  
Registration No. 25,426

SUGHRUE, MION, ZINN,  
MACPEAK & SEAS, PLLC  
2100 Pennsylvania Avenue, N.W.  
+Washington, D.C. 20037-3213  
Telephone: (202) 293-7060  
Facsimile: (202) 293-7860

Date: May 10, 2001

09831491:080801

09/831491

JC03 Rec'd PCT/PTC 10 MAY 2001

**PATENT APPLICATION**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of

Teow Hin NGAIR

Appln. No.: UNKNOWN

Group Art Unit: UNKNOWN

Confirmation No.: UNKNOWN

Examiner: UNKNOWN

Filed: May 10, 2001

For: A METHOD OF ENCRYPTION AND APPARATUS THEREFOR

**PRELIMINARY AMENDMENT**

Commissioner for Patents  
Washington, D.C. 20231

Sir:

Prior to examination, please amend the above-identified application as follows:

**IN THE CLAIMS:**

**Please enter the following amended claims:**

4. (Amended) A method as claimed in claim 1 further comprising the step of generating a session key for each symmetric key operation.

6. (Amended) A method as claimed in claim 4 wherein steps (a) and (b) are conducted recursively and the respective token signatures combined as a single combined token signature.

7. (Amended) A method as claimed in claim 4 further comprising the steps of:

- (i) processing the output data to generate a further input related to the output data;
- (ii) applying steps (a) and (b) to the further input to create a session bound output;
- (iii) combining the session bound output with the token bound output.

8. (Amended) A method as claimed in claim 1 wherein the user data or representation is split into a plurality of blocks and separate token signatures are generated for each block, the

09/831491 - 030001

token signatures being all combined with the user data or representation to generate the token bound output data.

9. (Amended) A method as claimed in claim 1 wherein the output data is used as an input parameter to a private key signature generation operation, to form a private key signature for the user data.

10. (Amended) A method of verifying token bound output data created by the method claim 1 by regenerating the token signature using the key employed to encrypt the data and matching it with that in the token bound output.

16. (Amended) Apparatus for performing the method of claim 1.

17. (Amended) Apparatus for performing the method of claim 10.

20. (Amended) A token as claimed in claim 18 being a smartcard.

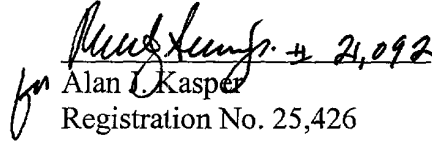
09531491.080807

**REMARKS**

Entry and consideration of this Amendment is respectfully requested.

Respectfully submitted,

SUGHRUE, MION, ZINN,  
MACPEAK & SEAS, PLLC  
2100 Pennsylvania Avenue, N.W.  
Washington, D.C. 20037-3213  
Telephone: (202) 293-7060  
Facsimile: (202) 293-7860

 2,092  
for Alan L. Kasper  
Registration No. 25,426

Date: May 10, 2001

09531491-030301  
T09030 T64T2960

## APPENDIX

### VERSION WITH MARKINGS TO SHOW CHANGES MADE

#### IN THE CLAIMS:

The claims are amended as follows:

4. (Amended) A method as claimed in ~~any one of claims 1 to 3~~ claim 1 further comprising the step of generating a session key for each symmetric key operation.

6. (Amended) A method as claimed in claim 4 ~~or 5~~ wherein steps (a) and (b) are conducted recursively and the respective token signatures combined as a single combined token signature.

7. (Amended) A method as claimed in ~~any one of claims 4 to 6~~ claim 4 further comprising the steps of:

- (i) processing the output data to generate a further input related to the output data;
- (ii) applying steps (a) and (b) to the further input to create a session bound output;
- (iii) combining the session bound output with the token bound output.

8. (Amended) A method as claimed in ~~any one of the preceding claims~~ claim 1 wherein the user data or representation is split into a plurality of blocks and separate token signatures are generated for each block, the token signatures being all combined with the user data or representation to generate the token bound output data.

9. (Amended) A method as claimed in ~~any one of the preceding claims~~ claim 1 wherein the output data is used as an input parameter to a private key signature generation operation, to form a private key signature for the user data.

10. (Amended) A method of verifying token bound output data created by the method of ~~any one of the preceding claims~~ claim 1 by regenerating the token signature using the key employed to encrypt the data and matching it with that in the token bound output.

16. (Amended) Apparatus for performing the method of ~~any one of claims 1 to 9 or 12~~ claim 1.

17. (Amended) Apparatus for performing the method of ~~any one of claims 10, 11, 13 or 14~~ claim 10.

20. (Amended) A token as claimed in claim 18 ~~or claim 19~~ being a smartcard.

09334491-030301

Rec'd PCT/PTO 10 MAY 2001

1

A METHOD OF ENCRYPTION AND APPARATUS THEREFORBACKGROUND AND FIELD OF THE INVENTION

5 This invention relates to a method of encryption and apparatus therefor, particularly for use with a token such as a smart card.

Smart cards, which contain onboard memory and computer  
10 processing ability are known. One application for such smart cards is for use as tokens for electronic transactions particularly in the banking sector. The card is used to "sign" a transaction digitally so that the instructed party (a bank in a funds transfer operation, for example) knows  
15 that the transaction is instructed by the holder of the card.

Such a transaction begins with the holder inserting the card into a suitable reader connected to a computer terminal in communication with the bank via a telephone line or the  
20 internet. The use of a PIN number known only to the holder grants initial access by the holder to the functions provided by the bank to the card holder. The holder can then instruct a transaction and the transaction is authenticated by a public/private key operation using the card. The card  
25 provides this by holding a private key of the holder and digitally signing the data. Subsequent verification by the bank using the holder's public key will identify that the

digitally signed instruction came from the holder's card unambiguously.

A disadvantage of transactions such as this is that current  
5 smart cards only have limited onboard processing power and  
since a private key operation requires high computational  
power, it is not feasible to provide the private key  
operation for the transaction in the card itself. Instead,  
this is performed by the terminal to which the card reader  
10 is connected. This requires that the private key be provided  
by the card to the terminal so that the operation may be  
performed. Once the private key has left the card, however,  
the security provided by the card will be at risk since the  
private key may be intercepted or copied. Once this has  
15 occurred, it is possible for the holder to be impersonated,  
since the private key relied upon for authentication of the  
transaction has been compromised.

It is an object of the invention to alleviate this  
20 disadvantage of the prior art.

#### SUMMARY OF THE INVENTION

According to the invention in a first aspect, there is  
25 provided a method of encryption for creating token bound  
output data from user data using a symmetric key capable  
token, said method comprising the steps of



- a. providing the user data or a representation thereof as an input to a symmetric key operation supported by the token,
- b. retrieving the output of the symmetric key operation as a token signature;and
- 5 c. combining the token signature with the user data or representation to generate the token bound output data.

Preferably said representation is a fingerprint of the user data, most preferably generated using a hash function

10

The method may further comprise the step of generating a session key for each symmetric key operation and the session key may be generated by modifying a symmetric key stored in the token number with a random number.

15

If a session key is employed, steps (a) and (b) may be conducted recursively and the respective token signatures combined as a single combined token signature and/or the method may further comprise the steps of:

- 20 (i) processing the output data to generate a further input related to the output data;
- (ii) applying steps (a) and (b) to the further input to create a session bound output;
- (iii) combining the session bound output with the token bound
- 25 output.

The user data or representation may also be split into a

T02020 Y54 F050

5

15

20 comprising the steps of:

- a. providing the user data or a representation thereof as an input to a symmetric key operation supported by the token;
- b. retrieving the output of the symmetric key operation as a token signature;
- 25 c. combining the token signature with the user data to generate token bound output data; and
- d. providing the output data as an input parameter to a

private key signature generation operation, to form a private key signature for the user data.

The method of the second aspect may further comprise the  
5 steps of using a signature verification operation to verify the token bound output data and re-generating the token signature using the symmetric key to verify the token.

The invention extends to apparatus for performing the above  
10 methods.

According to the invention in a third aspect, there is provided a token for an electronic transaction, the token supporting a symmetric key operation to generate a token  
15 signature from input data. Preferably, the token further stores a private key for a digital transaction signature operation and is embodied as a smartcard.

In the described embodiment, on-line symmetric key  
20 authentication of the smart card by a Secure Access Module is employed on top of a private/public key system. The former binds the transaction to the physical smart card that the user is holding. Thus, a two-layer security system is provided in which basic transaction-related operations are  
25 protected by the private/public key system and the symmetric key encryption binds these operations with the user's smart card. Hence, as long as at least one of these two security

09334494-0000004

schemes is not compromised, the resulting signature operation remains secure.

#### BRIEF DESCRIPTION OF THE DRAWING

5

An embodiment of the invention will now be described, by way of example, with reference to accompanying Figure 1 which is a schematic diagram of the main structural elements involved in an electronic transaction using the embodiment of the  
10 invention.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following detailed description, reference is made to  
15 a specific application of the invention using a Gemplus MPCOS (Multi Payment Card Operating System) smartcard and to use of existing features of this card to provide enhanced cryptographic security. It will be appreciated, however, that the invention is equally applicable for use with other  
20 smartcards and tokens generally.

With reference to Figure 1, a Gemplus MPCOS smartcard 10 is shown. The smartcard includes an onboard processor and memory chip 20 connected to data input/output terminals 30.  
25 The smartcard 10 is insertable in a reader 40 which includes contacts (not shown) which engage the terminals 30 thus allowing the card to communicate through the reader 40.

5

10

15

25

One method of creating such a smartcard signature for a MPCOS Smartcard is via the SELFK command using a card specific key K. More information on this secure messaging command may be found in the Gemplus "MPCOS-3DES Reference Manual".

5

A generic smartcard signature generation operation using SELFK command has the following steps:

1. The terminal software generates a 8-byte number R, which  
10 is essentially random, such as a hash value of user data.
2. The terminal sends the command SELFK(R, Kindex) to the MPCOS card to generate a card signature, where Kindex indicates the secret symmetric key K held by the card to be  
15 used for encryption (the card may have several keys, each having a different Kindex).
3. Upon receipt of the instruction, the MPCOS card generates a 8-byte random number CR. The MPCOS card then  
20 computes a session key:  $TK = 3DES(CR, K)$ , by applying a triple DES operation to CR using K. and generates an encrypted output signature:  $S = 3DES(R, TK)$ , by applying a triple DES operation to R using session key TK.
- 25 4. The terminal retrieves both the smartcard signature S and card random number CR.

T00000"64T0000

To verify the signature S based on R and CR, the bank sends these values together with the card serial number (CSN) and Kindex to the SAM 70 which securely holds the symmetric keys associated with the card to re-compute the value of S. If the  
5 two S values do match, the bank can be sure that the MPCOS card with the CSN serial number is indeed present. To prevent misuse, the comparison of the S values should only be done in the SAM 70 itself. The comparison result is then output to the bank computer 60.

10

To achieve this verification, the SAM 70 needs to store the card specific key K. Since many keys for different cards  
10 will need to be stored, the SAM 70 may hold a master key, from which all the specific keys K can be derived. The SAM  
15 70, however, needs to be held in a secure environment, for example in the data centre of the bank or other secure premises and guarded with a sound and secure policy.

In actual implementation, the MPCOS card only outputs the 4  
20 least significant bytes of S as a security measure. Therefore, only the 4 least significant bytes are sent by terminal 40 and compared by the SAM 70. However, 4 bytes of signature S may not provide sufficient security strength to prevent an exhaustive search attack. The signature algorithm  
25 is preferably, therefore, extended as follows:

1. The terminal software generates the number R.
2. Loop for j from 1 to n, do 2a-2f.
  - 2a. The terminal sends the command SELFK(R, Kindex) to the MPCOS card.
  - 5 2b. The MPCOS card generates a 8-byte random number CR
  - 2c. The MPCOS card computes  $TK = 3DES(CR, K)$ , and output  $S = 3DES(R, TK)$ .
  - 2d. The terminal retrieves both the 4 byte output value S and 8-byte card random number CR.
  - 10 2e. The terminal concatenates S to an initially empty buffer S', and similarly concatenates CR to an initially empty buffer CR'.
  - 2f. Loop back to 2a with R now set to a hash function-derived value  $H(R||S||CR)$ , where || represents concatenation.
- 15 Using the above algorithm, cryptogram S' can have any length, depending upon the number of iterations n and can be used as the MPCOS card signature of the input value R. The signature S' is notionally divided into n four byte elements and  
20 corresponding n eight byte elements of random number CR'.

To provide the required verification, the SAM 70 then repeats the algorithm noted using the initial input R, the elements of CR' and the hash function H to generate and verify the  
25 elements of S'. For commercial grade security, S' should preferably have a length of at least 128-bits. This can be achieved by setting the loop number n in step 2 to 4.



5

10

15

20

As in the prior art, the smartcard does not have sufficient computing power to perform the private key operation. Therefore, the private key is output from the card to the terminal 50 which computes the private key operation which generates the digital transaction signature before sending this to the bank computer 60 together with the document, the token signature, the card serial number (CSN) and Kindex.

10 The bank computer 60 then performs a public key operation using the document transaction signature, the user's public key, the smartcard signature and the document, to verify the document transaction signature. The bank then generates the hash function fingerprint  $h(D)$  of the document. The  
15 smartcard signature  $S(R)$ , card serial number CSN and the hash function fingerprint  $h(D)$  are then sent to the SAM 70 which performs the symmetric encryption operation on  $h(D)$  using the symmetric key it holds and CR (CR') from the card signature and compares the result with S (S') from the card  
20 signature to determine if the signature came from the card identified by the card serial number. If so, an indication is given to the bank computer 60 thus providing a verification that the transaction was conducted with the physical presence of the card 10.

25

Usually, the length of  $h(D)$  is longer than the 8-byte number R needed for generating the smart card signature. To use the

T08080" T04T E860

whole of  $h(D)$  and increase the security strength of the smart card signature further,  $h(D)$  can be split into 8-byte blocks of  $h(D)_1, \dots, h(D)_m$  (discarding any incomplete trailing block) with each block being processed independently. These  
 5 processed blocks are then concatenated so that the transaction signature is modified to  $p(h(D) || S(h(D)_1) || \dots || S(h(D)_m))$ .

Each block can be processed to form a concatenated signature  
 10  $S'$  as discussed above. The loop count 2a-2f above for each  $S'$  can be correspondingly reduced to balance between security and data length.

To verify the digital signature generated with the above it  
 15 is necessary to transmit the additional values of  $S$  and  $CR$  (or  $S'$  and  $CR'$ ) for each element  $S(h(D)_1) - S(h(D)_m)$  of the smart card signature generated. The verification application of the bank computer 60 will then check the value of each  $S(h(D)_i)$  ( $i = 1$  to  $m$ ) against each pair of  $h(D)_i$  and  $CR$  using  
 20 the SAM 70 for computation of each  $S$  value.

One potential weakness to the above method is that even though a security mechanism is included to ensure that the digital signature is generated with a prior access to the  
 25 appropriate smartcard, it is not possible for the bank to tell that the smartcard signature is generated during the same session as the digital transaction signature. For

example, whenever the smartcard is inserted into a compromised computer, an attacker could possibly generate many smart card signatures with different documents and store them. At a later point when the attacker discovers the user's private key, the correct digital transaction signatures can then be generated without accessing the smart card.

A variation of the method using the following steps can prevent such an attack, by providing a means for the smartcard to encrypt an input related to the signature with the card's session key:

1. Create a file in the Smartcard memory.
- 15 2. Create a PIN number to protect access to the file
3. Set the file update permission to allow any application to write to the file in plain text.
4. Set the file read permission to allow MPCOS secure messaging [i.e. encrypted messaging] only.

20

With such a smart card file, a cryptogram can be generated from the MPCOS card that assures that the digital transaction signature is generated during the same session as the last SELFK command used to create the smartcard signature using the following steps:

1. Do not reset the card after the last SELFK command that

2. After the  $p$  signing operation, generate a hash  $m$  of the digital transaction signature.

5

5. Read back the value of  $m$  using the MPCOS RDBIN (read binary file) command with secure messaging, that is

The value read in step 5 is added to the digital transaction signature. The SAM 70 then checks encrypted value  $m$  as part of the smartcard signature verification routine. With this enhancement, a positive verification by the SAM 70 securely indicates that the public key signature is indeed generated during one single smart card session.

The embodiment described is not to be construed as  
20 limitative. For example, the invention is applicable to  
other kinds of tokens other than smartcards such as a PCMCIA  
token. The token signature generating method can be used on  
its own or with other encryption or digital signing  
techniques, not limited to public/private key operations for  
25 digital transaction signature generation as described.

CLAIMS

1. A method of encryption for creating token bound output data from user data using a symmetric key capable token, said  
5 method comprising the steps of
- a. providing the user data or a representation thereof as an input to a symmetric key operation supported by the token,
  - b. retrieving the output of the symmetric key operation as the token signature; and
- 10 c. combining the token signature with the user data or representation to generate the token bound output data.
2. A method as claimed in claim 1 wherein said representation is a fingerprint of the user data.
- 15 3. A method as claimed in claim 2 wherein the representation is generated using a hash function
4. A method as claimed in any one of claims 1 to 3 further  
20 comprising the step of generating a session key for each symmetric key operation.
5. A method as claimed in claim 4 wherein the session key is generated by modifying a symmetric key stored in the token  
25 with a random number.



5

10

15

- 20

25



14. A method as claimed in claim 13 wherein the token  
5 signature is verified at a secure location at which the  
symmetric key is stored.

10

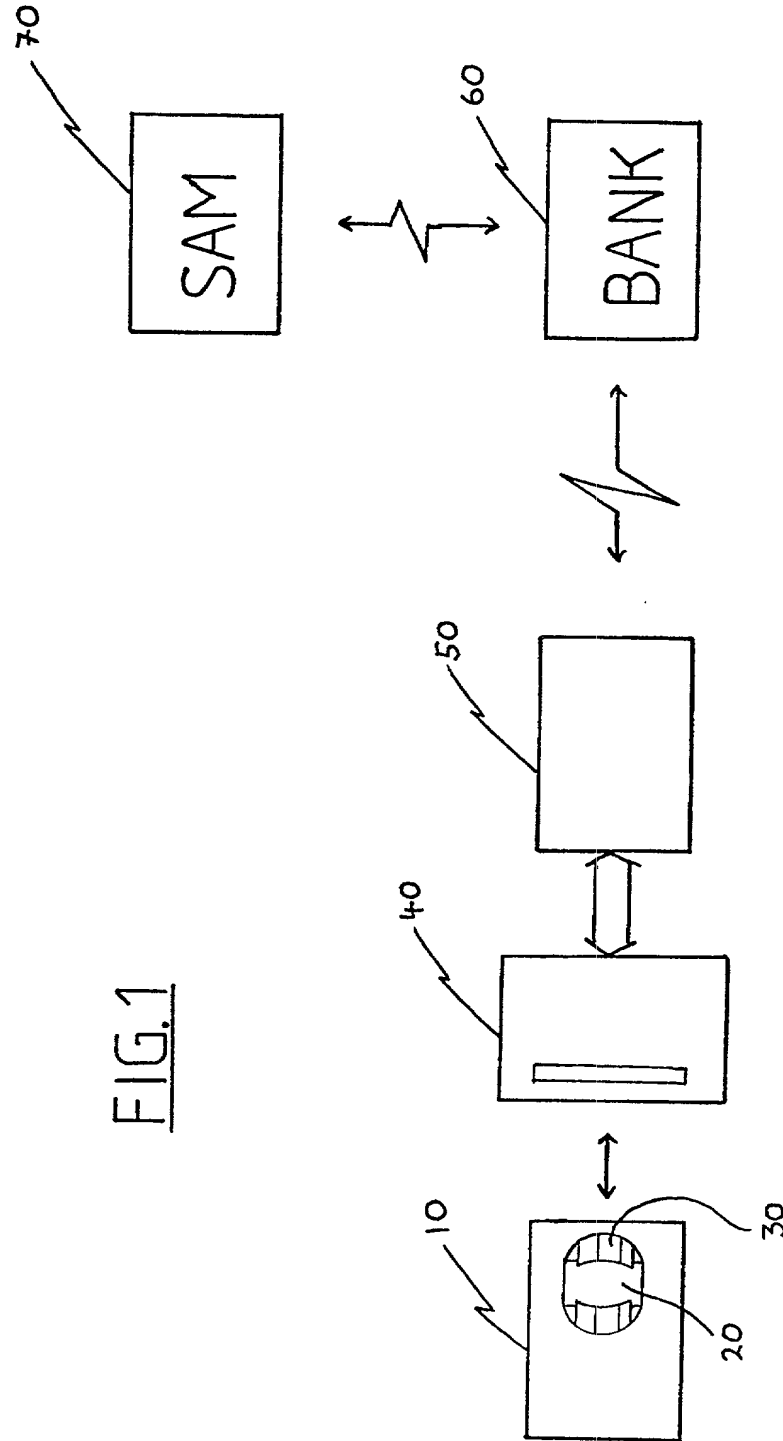
15

18. A token for an electronic transaction, the token supporting a symmetric key operation to generate a token signature from input data.

19. A token as claimed in claim 18 wherein the token further stores a private key for a digital transaction signature operation.

25 20. A token as claimed in claim 18 or claim 19 being a smartcard.

1/1



SOLE/JOIN  
Q644C**DECLARATION AND POWER OF ATTORNEY**

As a below named inventor, I hereby declare that my residence, mailing address and citizenship are as stated below next to my name that I verily believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (plural names are listed below) of the subject matter claimed and for which a patent is sought in the application entitled:

**A METHOD OF ENCRYPTION AND APPARATUS THEREFOR**

which application is:  
☐ the attached application  
 (for original application)

PCT Application No. PCT/SG98/00088  
☒ Application No. 09/831,491  
 (Confirmation No. ) filed Nov. 10, 1988,  
 and amended on

(for declaration not accompanying application)

that I have reviewed and understand the contents of the specification of the above-identified application, including the claims, as amended by any amendment referred to above; that I acknowledge my duty to disclose information of which I am aware and which material to the patentability of this application as defined in 37 C.F.R. 1.56, that I hereby claim priority benefits under Title 35, United States Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, §119(e) of any United States provisional application(s), or §365(a) of any PCT International application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate or of an PCT International application having a filing date before that of the application on which priority is claimed:

Application Number	Country	Filing Date	Priority Claimed	
			Yes	No

I hereby claim the benefit under 35 United States Code §120 of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in a listed prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge my duty to disclose any information material to the patentability of this application as defined in 37 C.F.R. 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application No.	Filing Date	Status

I hereby appoint John H. Mion, Reg. No. 18,879; Thomas J. Macpeak, Reg. No. 19,292; Robert J. Seas, Jr., Reg. No. 21,092; Darrin A. Olexy, Reg. No. 23,063; Robert V. Sloan, Reg. No. 22,775; Peter D. Olexy, Reg. No. 24,513; J. Frank Osha, Reg. No. 24,621; Waddell A. Biggart, Reg. No. 24,861; Louis Gubinsky, Reg. No. 24,835; Neil B. Siegel, Reg. No. 25,200; David J. Cushing, Reg. No. 25,703; John R. Inge, Reg. No. 26,916; Joseph J. Ruch, Jr., Reg. No. 26,577; Sheldon I. Landsman, Reg. No. 25,430; Richard C. Turner, Reg. No. 29,710; Howard L. Bernstein, Reg. No. 25,665; Alan J. Kasper, Reg. No. 25,426; Kenneth J. Burchfiel, Reg. No. 31,333; Gordon Kit, Reg. No. 30,764; Susan J. Mack, Reg. No. 30,951; Frank L. Bernstein, Reg. No. 31,484; Mark Boland, Reg. No. 32,197; William H. Mandir, Reg. No. 32,156; Brian W. Hannon, Reg. No. 32,778; Abraham J. Rosner, Reg. No. 33,276; Bruce I. Kramer, Reg. No. 33,725; Paul F. Neils, Reg. No. 33,102; Brett S. Sylvester, Reg. No. 32,765; Robert M. Masters, Reg. No. 35,601; George F. Lehnigk, Reg. No. 36,359; John T. Callahan, Reg. No. 32,607; Steven M. Gruskin, Reg. No. 36,818; Peter A. McKenna, Reg. No. 38,551 and Edward F. Kenehan, Reg. No. 28,962, my attorneys to prosecute this application and to transact all business with the Patent and Trademark Office connected therewith, and request that all correspondence about the application be addressed to **SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC**, 2100 Pennsylvania Avenue, N.W., Washington, D.C. 20037-3213.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Date 19 June 2001 First Inventor Teow Hin NGAIR  
 Residence 334 Kang Ching Road #13-254 Singapore 610334  
 City Singapore State/Country Singapore  
 Mailing Address: 334 Kang Ching Road #13-254  
Singapore 610334  
 Citizenship Singapore